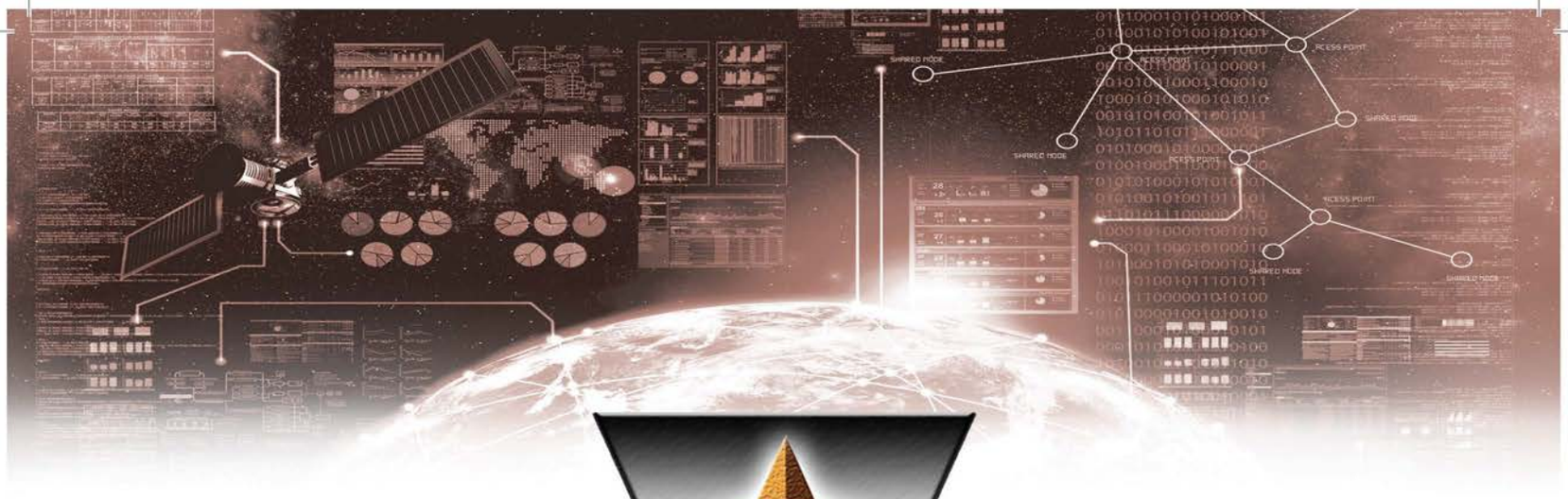


SPAWAR
Systems Center
PACIFIC

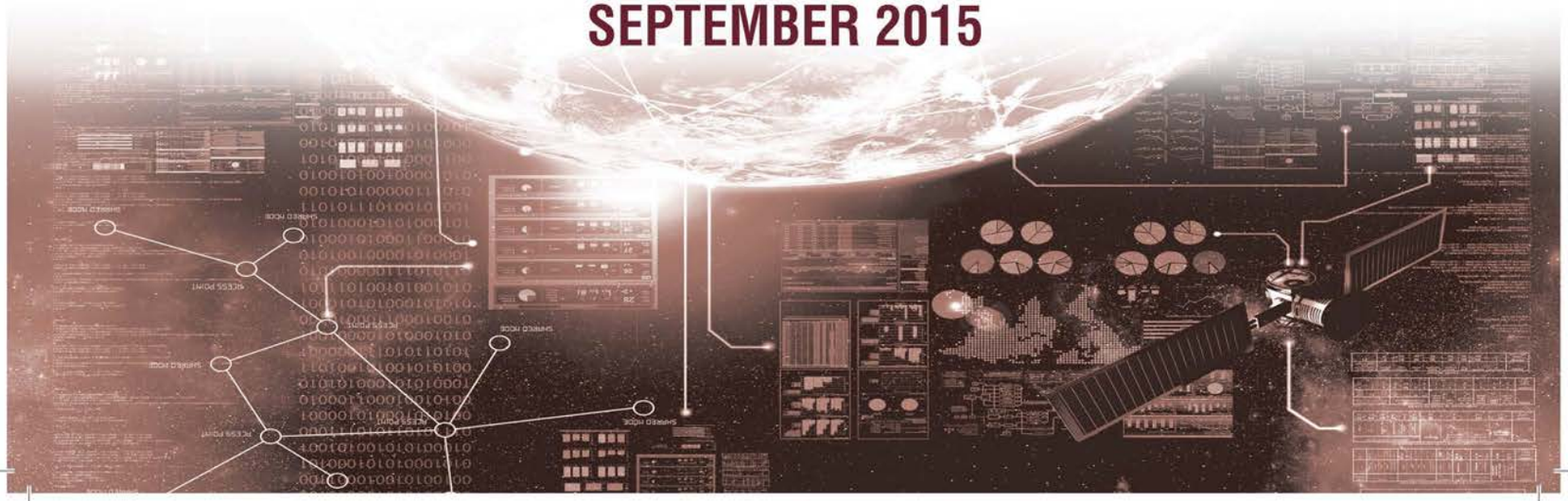
EUCOM KEYSTONE

Connecting Across Services Enabling Timely Horizontal & Vertical Integration

PRODUCT REFERENCE GUIDE

REVISION 1.0

SEPTEMBER 2015



Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
SEP 2015		**00-00-2015 to 00-00-2015**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
EUCOM Keystone: Connecting Across Services Enabling Timely Horizontal & Vertical Integration, Product Reference Guide, Revision 1	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **SSC Pacific, 53560 Hull Street,,San Diego,,CA, 92152**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT
This document describes the EUCOM Keystone products and related non-material solutions. Further, this document provides information for obtaining Keystone products and support. Lastly, the document contains artifact information for use in the Defense Technical Information Center (DTIC) for future programs and products.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**65**	

TECHNICAL DOCUMENT 3299
September 2015

EUCOM KEYSTONE PRODUCT REFERENCE GUIDE Revision 1

Douglas R. Hardy
SSC Pacific

Christopher E. Russell
Patricia C. Hile
Global Systems Engineering
G2 Software Systems, Inc.

SSC Pacific
San Diego, CA 92152-5001

SSC Pacific
San Diego, California 92152-5001

K. J. Rothenhaus, CAPT, USN
Commanding Officer

C. A. Keeney
Executive Director

ADMINISTRATIVE INFORMATION

This work was prepared by the Command and Control (C2) Interoperability and Information Systems Branch (Code 53627) of the C2 Technology and Experimentation Division (Code 53600), Space and Naval Warfare Systems Center Pacific (SSC Pacific), San Diego, CA. The Physical Security Enterprise & Analysis Group (PSEAG) under the Office of the Deputy Assistant Secretary of Defense for Nuclear Matters provided funding for this project.

Released by
E. Nguyen, Head
C2 Interoperability &
Information Systems Branch

Under authority of
C. Raney, Head
C2 Technology &
Experimentation Division

SB

Contents

Figures

1 Introduction

The tragic shootings at Fort Hood in November 2009, the Washington Navy Yard in September 2013, and again Fort Hood in April 2014 have underscored the need to improve information sharing with partner agencies and among installations across the U.S. areas of responsibility. During the first two events (findings from the most recent Fort Hood incident are still being analyzed), installations in the surrounding area were not notified, nor was U.S. Northern Command (USNORTHCOM). Had either of these shootings been part of a coordinated attack, U.S. installations were unprepared to change their force protection posture. In response, USNORTHCOM developed a national information sharing-middleware to change this dynamic. Across the country, organizations are able to overcome technical challenges and institutionalize information-sharing across disparate government and commercial emergency management and force protection systems. However, the same needs have been defined in the U.S. European Command (EUCOM) and other Combatant Commands Integrated Priority Lists (IPLs). Within the EUCOM area of responsibility, there are limited force protection processes and procedures that facilitate the sharing of automated, near real-time, event information among Outside Continental United States (OCONUS) commands and Host Nation First Responders. Currently, EUCOM cannot pass automated, timely, force protection, threat, and emergency management information to enable Host Nation First Responders to aid in the deterrence, interdiction, and the defeat of threats.

1.1 The EUCOM Keystone Project Mission

EUCOM Keystone is a Physical Security Enterprise and Analysis Group (PSEAG)-funded, joint initiative to establish near real-time information-sharing interfaces across currently "stove-piped" unclassified force protection and emergency management (FP/EM) applications through the use of middleware (Keystone). Its purpose is to enhance automated information sharing with Host Nation First Responders to enable continued mission assurance. The solution shall neither require the adoption of a new system or end-user hardware/tools nor replace already existing capabilities. Keystone facilitates dissemination of time-critical incident, imminent threat, and/or hazard information within the EUCOM area of responsibility to make the information-sharing process more efficient through automation.

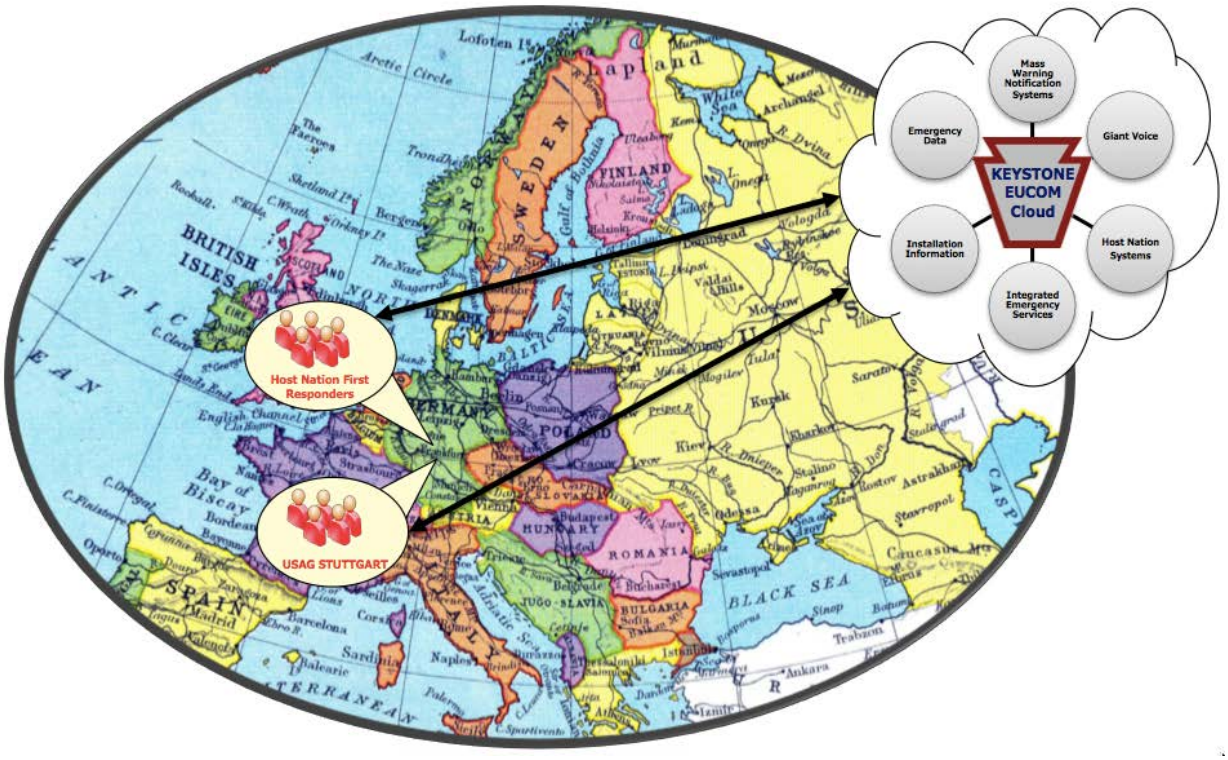


Figure 1: EUCOM Keystone improves alerting capability and response time in EUCOM AOR

EUCOM Keystone improves alerting capability and response time between the OCONUS Department of Defense (DoD) Garrison and Host nation.

1.2 The Keystone Solution

EUCOM Keystone is based on the Mission Assurance, Threat Alert, Disaster Resiliency and Response (MATADRR) project that transitioned an EM information sharing-capability named Keystone to the Emergency Management and Modernization Program (EM2P), a program office within the Joint Program Executive Office for Chemical and Biological Defense's (JPEO CBD) Joint Program Manager Guardian (JPMG).

Keystone is a standards-based middleware that receives, translates, and transmits incident-related data between linked disparate systems to allow a common view between them. As middleware, Keystone does not interface directly with end-users. Keystone is the transporter of uniform data in common formats. Emergency applications (sensors, incident logs, personnel management, dispatch systems, video surveillance and intelligence tools – anything related to homeland security) can provide a portion of their data to Keystone, which then publishes it to subscribers' applications. The applications then see the consumed data inside their own user interface. Thus, to the user, there is no new application, no new learning, and no conscious sending of information. Further, Keystone is not intended to replace current standard operating procedures, messages and/or reports for communicating emergency management and force protection data. It is intended to

enhance, enable and more quickly disseminate emergency management and force protection data to a broader community of recipients. Paramount to Keystone's success is the concept of improved local and regional awareness, with simultaneous national and international awareness, available to decision makers at all levels in between.

By using data standards, by managing data content, by ensuring two-way sharing of data, by protecting data ownership, and by defining the minimal fraction of data needed for collaborative decision-making, Keystone is allowing organizations to work within their own existing concepts of operations (CONOPS) using their own prior technology investments to achieve information sharing.

1.3 Purpose

This document describes the EUCOM Keystone products and related non-materiel solutions. Further, this document provides information for obtaining Keystone products and support. Lastly, the document contains artifact information for use in Defense Technical Information Center (DTIC) for future programs and projects.

2 Transition Products

The goal of EUCOM Keystone is to share information across domains, roles, functions, hazards, and applications—not to create a new application that everyone must use. The EUCOM Keystone project uses the Keystone software to provide true information sharing among applications that enables each individual application – selected for its intrinsic value by an end-user organization – to acquire common data and compose that data into a visualization that is appropriate for the end-user (Figure 2). The application then can further process that data and resubmit it for sharing with the originating – and other interested – applications. Keystone is not one size fits all; one application cannot meet all needs. Keystone builds many-to-many relationships among applications to meet the unique needs of very diverse end-user communities created by the CONOPS the communities construct.

Figure 2: EUCOM Keystone Operational View

2.1 Keystone Architecture Overview

The Keystone architecture is constructed of two main web services: the Core and the software adapters (Figure 3). The Core manages infrastructure and services while the software adapters perform the actual translations. The architecture is built on service-oriented principles using open standards. Each Keystone Core serves as a local point of integration. Keystone Cores support three varieties of services: infrastructure, domain, and external. Infrastructure services enable the sharing of information between Cores and are based on existing, established industry standards. Domain services provide for the sharing of translated information specific to EM/FP; such as all hazards and threats, incidents, command hierarchies, tasking, and shared awareness. These services rely on existing and developing standards in the EM/FP domains – such as those from National Information Exchange Model (NIEM) and the Organization for the Advancement of Structured Information Standards (OASIS) EM Technical Committees. In addition each, Core provides the ability to register external services using existing, developing and future standards.

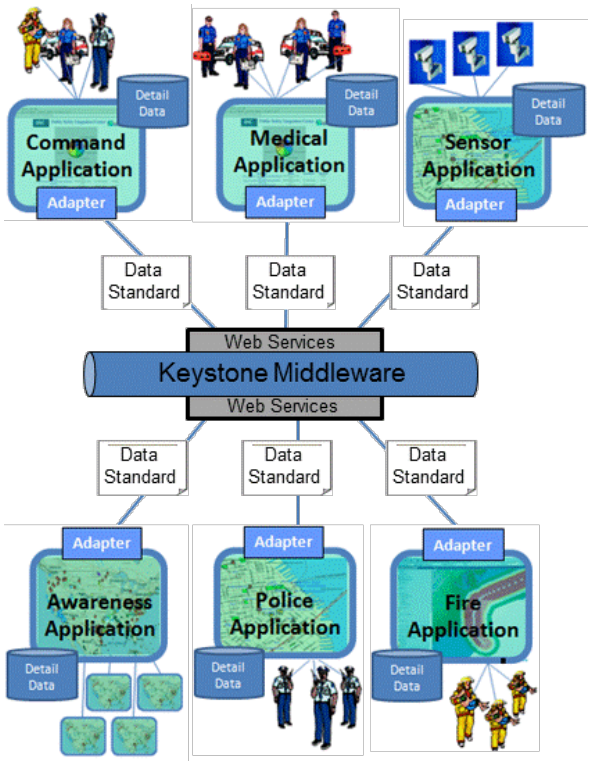


Figure 3: Keystone Architecture

2.1.1 Scalability

A valuable feature of the Keystone architecture is its scalability. That is, Keystone can be modified to serve any type or size of community. The Keystone Core can be deployed as a simple stand-alone system for a few sites or as a system of distributed networked Cores.

Contact Information

Operational Manager

EUCOM

Joe Fagan

Joe.e.fagan.civ@mail.mil

49 711 680-8955

Transition Manager

SPAWARSYSCENPAC

Doug Hardy

Douglas.hardy@navy.mil

619-553-5410

Deputy Transition Manager

GSE

Chris Russell

Chris.russell@globalsyseng.com

703-915-2338

Technical Manager/Performer

ARDEC

Italo Grasso

Italo.g.grasso.civ@mail.mil

973-724-8052

2.2 Keystone Core

Technology Readiness Level: **7+**

Deliverables: **Source code, software executable files, business rules, documentation and information assurance data**

2.2.1 Description

As stated previously, the Keystone Core manages domain services and infrastructure services. Domain services include incident management, incident commands, incident action plans, tasking, alerts, maps, resources, and sensors. Infrastructure services include agreements, profiles, notifications, work products, directories, and broadcasts.

The Cores are configured to support agreements, for the exchange of data. Agreements follow local Memorandums of Understanding (MOUs) and/or Mutual Aid Agreements (MAAs) that define the terms and conditions under which service component installations will share information. Agreements must be mutually established prior to data-sharing and enable dynamic, all hazards and threats data sharing topologies.

2.2.2 Deployment

Keystone Cores can be installed on any virtual machine and network depending on the governance and policies of the participating organizations. Cores can be hosted by a government agency for several other agencies or Core hosting can be outsourced for those sites that do not have the requisite information technology infrastructure.

2.3 Keystone Adapters and Interfaces

2.3.1 Description

Keystone adapters perform the following functions:

- Provide two-way information sharing among commercial and government incident management technologies to achieve collaborative decision-making
- Correlate information from all these sources into defined incidents, meaning that all relevant information about an incident can be available from one source—Keystone
- Provide content management for information associated with incidents so that connected applications know that they are getting the latest, authoritative source data available

2.3.2 How It Works

When an organization installs Keystone, it sets up secure sharing exchange agreements that define how and with whom it will share its information. Data owners continue to compose their data as usual within their own specific system/domain. Keystone then builds a defined incident about an event by compiling a series of Keystone Work Products composed of data provided by applications interfaced to Keystone through the application's Keystone Adapter. The adapter authenticates the application to connect to Keystone Web Services and translates the detailed data of the application into the fractional data in a standard format to be shared through Keystone. Thus, the Keystone Work Product is the basic unit of data exchange among applications. Each application provides data when it has something to contribute to the incident knowledgebase and consumes a work product when it wants its end-user to know about the incident.

All adapters can reside on an Enterprise Service Bus (ESB) that provides support for messaging reliability, security, performance, and translation to and from standard formats, such as, the Common Alerting Protocol (CAP), the National Incident Management System (NIMS) and the National Information Exchange Model (NIEM). New adapters can easily be added using the Software Development Kit (SDK).

2.3.3 EUCOM Keystone Interfaces and Adapters

A number of adapters and interfaces have already been developed[1], the adapters used in the EUCOM Keystone project included:

- GeoByte
- AtHoc
- WebEOC
- SAGE
- PSIF

Other adapters exist and are listed here:

- C4IS
- ICD-0101B (prototype, sensors)
- JIEE
- C2PC (prototype)

[1] Development of adapters to commercial products does not define an endorsement by the Government for these systems.

Contact Information

Operational Manager

EUCOM

Joe Fagan

Joe.e.fagan.civ@mail.mil

49 711 680-8955

Transition Manager

SPAWARSYSCENPAC

Doug Hardy

Douglas.hardy@navy.mil

619-553-5410

Deputy Transition Manager

GSE

Chris Russell

Chris.russell@globalsyseng.com

703-915-2338

Technical Manager/Performer

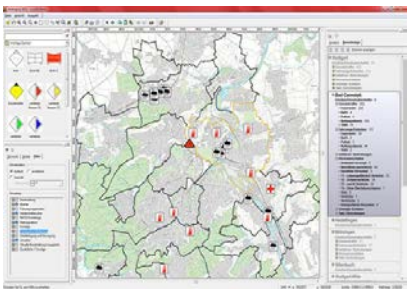
ARDEC

Italo Grasso

Italo.g.grasso.civ@mail.mil

973-724-8052

2.3.4 GeoByte Adapter



Technology Readiness Level: **6+**

Deliverables: **Source code, software executable files, documentation**

Description

GeoByte is an emergency management system used in the Stuttgart area, many other cities / counties in Germany and Austria, the Grande Duchy of Luxembourg as well as several ministries in German Federal States. Specific to the objective of Keystone, GeoByte has its own "InterConnect Server" to exchange incident information between cities, counties, ministries and between fire departments, emergency agencies and police forces. GeoByte interfaces existing control center applications to retrieve basic information about incidents, offers functions like networked common operational pictures, communications diagrams, and summarized information for area-wide disasters like flood and storm hazards plus a communication module supporting common standards such as ICS (Incident Command System) –networking operatives on the ground and allowing overall management of incidents. GeoByte also contains planning and preparedness modules designed for implementing EM simulations and exercises.

Client Type

HTTPS

Data Format

XML and EDXL

Communication Flow

- Keystone to Host nation EM/FP
- Within GeoByte metropoly NEO (Networked Emergency Operations) there is a communication flow between the GeoByte Server, mobile command units and emergency operations centers.

Contact Information

Operational Manager

EUCOM

Joe Fagan

Joe.e.fagan.civ@mail.mil

49 711 680-8955

Transition Manager

SPAWARSYSCENPAC

Doug Hardy

Douglas.hardy@navy.mil

619-553-5410

Deputy Transition Manager

GSE

Chris Russell

Chris.russell@globalsyseng.com

703-915-2338

Technical Manager/Performer

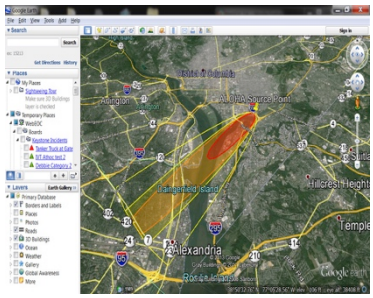
ARDEC

Italo Grasso

Italo.g.grasso.civ@mail.mil

973-724-8052

2.3.5 WebEOC Adapter



Technology Readiness Level: **7+**

Deliverables: **Source code, software executable files, Army suggested business rules, documentation and information assurance data**

Description

WebEOC® is a web-enabled and locally configurable incident and event management system. With access to the Internet, authorized emergency managers and first responders, regardless of location, can enter and view incident information in WebEOC status boards. WebEOC enables users to manage multiple incidents and daily events, assign and track missions and tasks, provide situation reports, manage resources, and prepare Incident Command System (ICS) and Incident Action Plan (IAP) reports. WebEOC is used by federal, state, county and city entities.

Client type

HTTP Polling

Data Format

WebEOC XML

Communication Flow

- Create/update incidents
- Incident sharing
- Plume sharing
- Bidirectional
    - WebEOC to Keystone Core
    - Keystone Core to WebEOC

Contact Information

Operational Manager

EUCOM

Joe Fagan

Joe.e.fagan.civ@mail.mil

49 711 680-8955

Transition Manager

SPAWARSYSCENPAC

Doug Hardy

Douglas.hardy@navy.mil

619-553-5410

Deputy Transition Manager

GSE

Chris Russell

Chris.russell@globalsyseng.com

703-915-2338

Technical Manager/Performer

ARDEC

Italo Grasso

Italo.g.grasso.civ@mail.mil

973-724-8052

2.3.6 PSIF Adapter

Technology Readiness Level: **7+**

Deliverables: **Source code, software executable files, Army suggested business rules, documentation and information assurance data**

Description

The Physical Security Integration Framework (PSIF) is an emergency response and information management system focused on the incident command post (ICP) to emergency operations center interface with "All-Hazards" capable functionality. PSIF provides an integration platform that facilitates interoperability and provides a common operating picture (COP) that enables situational awareness for on scene response and off scene support personnel during all phases of incident management activities. The primary operators of the system are Department of Defense (DoD) civilians to include installation emergency management personnel, decision makers and first responders.

Client Type

Current R14.01 (PSIF V7.1.2)
PSIF->Keystone http connection, REST interface
Keystone->PSIF http connection, REST interface
R14.06 proposed (PSIF V7.2.0)
PSIF->Keystone jms connection, tcp over SSL, JAXB interface, pub/sub topics - client to broker
Keystone->PSIF jms connection, tcp over SSL, JAXB interface, pub/sub topics - broker to client

Data Format

R14.01
PSIF XML *(see PSIF API documents for object model)*
R14.06 proposed
JAXB messaging objects *(see PSIF JAXB data model)*

Communication Flow

- Create/update incidents
- Incident sharing
- Plume sharing
- Bidirectional
    - PSIF to Keystone Core
    - Keystone Core to PSIF

Contact Information

Operational Manager

EUCOM

Joe Fagan

Joe.e.fagan.civ@mail.mil

49 711 680-8955

Transition Manager

SPAWARSYSCENPAC

Doug Hardy

Douglas.hardy@navy.mil

619-553-5410

Deputy Transition Manager

GSE

Chris Russell

Chris.russell@globalsyseng.com

703-915-2338

Technical Manager/Performer

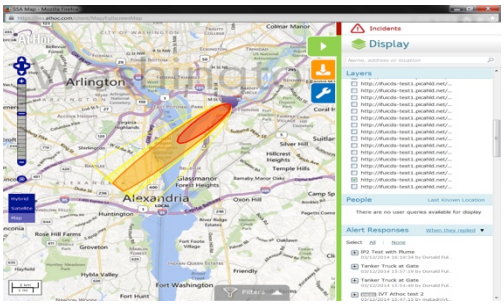
ARDEC

Italo Grasso

Italo.g.grasso.civ@mail.mil

973-724-8052

2.3.7 AtHoc Adapter



Technology Readiness Level: **7+**

Deliverables: **Source code, software executable files, documentation and information assurance data**

Description

AtHoc IWSAlerts™ provides enterprise-class, network-centric mass notification and emergency communication systems customized for military, government, healthcare, higher education and commercial organizations. The AtHoc solutions automate the end-to-end emergency communication process, delivering physical security, force protection, situational awareness, and personnel accountability. Allow communication between AtHoc and other Emergency Management Systems via Keystone.

Client type

AtHoc -> Keystone: HTTP Post to AtHoc SDK (polling)
Keystone -> AtHoc: HTTP Post to AtHoc SDK

Data Format

AtHoc XML: see AtHoc SDK Manual

Communication Flow

- Create/update incidents
- Incident sharing
- Plume sharing
- Bidirectional
    - AtHoc to Keystone Core
    - Keystone Core to AtHoc

Contact Information

Operational Manager

EUCOM

Joe Fagan

Joe.e.fagan.civ@mail.mil

49 711 680-8955

Transition Manager

SPAWARSYSCENPAC

Doug Hardy

Douglas.hardy@navy.mil

619-553-5410

Deputy Transition Manager

GSE

Chris Russell

Chris.russell@globalsyseng.com

703-915-2338

Technical Manager/Performer

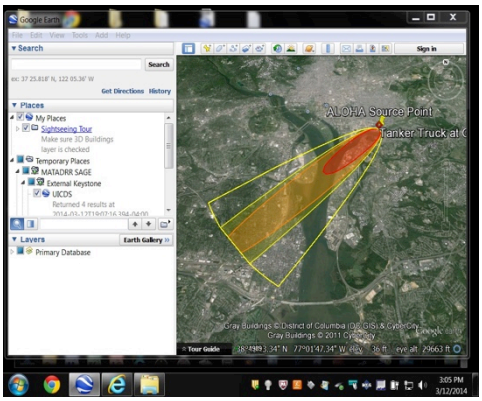
ARDEC

Italo Grasso

Italo.g.grasso.civ@mail.mil

973-724-8052

2.3.8 SAGE Interface



Technology Readiness Level: **7+**

Deliverables: **Source code, software executable files, USNORTHCOM suggested business rules, documentation and information assurance data**

Description

US Northern Command's SAGE (Situational Awareness Geospatial Enterprise) bridges the gap between disparate situational awareness systems by integrating critical infrastructure, force tracking, interagency, and incident management data at the unclassified, NIPRnet level. USNORTHCOM has taken a full service oriented architecture (SOA) approach to providing data both at USNORTHCOM headquarters and throughout the unclassified DoD community in support of Homeland Defense and Homeland Security efforts.

SAGE is a robust Geographic Information System (GIS) architecture designed to distribute and empower all USNORTHCOM Mission Partners with actionable geospatial data anywhere in the world. Keystone implants the Google Earth KML (Keyhole Markup Language) publishing interface to consume the Keystone Work Product sharing.

Client type

Google Earth KML interface

Data Format

Consume Keystone Work Product XML data format

Communication Flow

Unidirectional: Keystone Core to SAGE

Contact Information

Operational Manager

EUCOM

Joe Fagan

Joe.e.fagan.civ@mail.mil

49 711 680-8955

Transition Manager

SPAWARSYSCENPAC

Doug Hardy

Douglas.hardy@navy.mil

619-553-5410

Deputy Transition Manager

GSE

Chris Russell

Chris.russell@globalsyseng.com

703-915-2338

Technical Manager/Performer

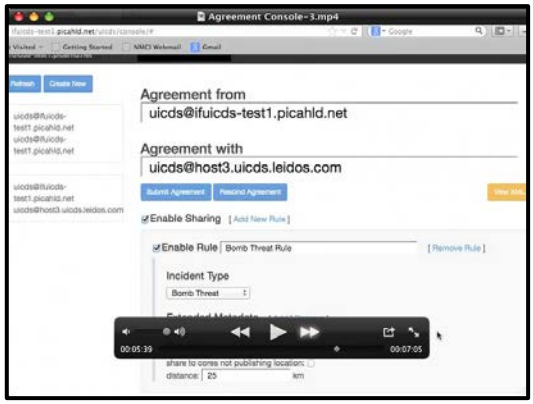
ARDEC

Italo Grasso

Italo.g.grasso.civ@mail.mil

973-724-8052

2.4 Keystone Administrative Console/Agreement Services



Technology Readiness Level: **6+**

Deliverables: **Source code, software executable files, business rules, and documentation**

Description

The Administrative Console is the graphical user interface to the Keystone Core for system administrators. It provides the means to establish and define relationships between Keystone Cores and Keystone Adapters through their associated incident management applications. An administrator can create resource profiles to allow subscription to the data in the Core; setup sharing agreements between multiple Cores; display, close and archive incidents and work products; and monitor the health and status of the Core.

Agreement services are enabled through the Administrative Console. Agreement services include sharing data by:

1) incident/event type,
2) specified incident,
3) proximity (range), and
4) specific metadata.

The agreement services are normally predefined and allow information sharing relationships based on mutual aid agreements, memorandums of agreements, memorandums of understanding, and other contractual documents between organizations.

Contact Information

Operational Manager

EUCOM

Joe Fagan

Joe.e.fagan.civ@mail.mil

49 711 680-8955

Transition Manager

SPAWARSYSCENPAC

Doug Hardy

Douglas.hardy@navy.mil

619-553-5410

Deputy Transition Manager

GSE

Chris Russell

Chris.russell@globalsyseng.com

703-915-2338

Technical Manager/Performer

ARDEC

Italo Grasso

Italo.g.grasso.civ@mail.mil

973-724-8052

2.5 Keystone Software Development Kit (SDK)

2.5.1 SDK Request

To request a copy of the current SDK release, please send an email to the Keystone Product Support List, usarmy.pica.rdecom.list.keystone-product-support@mail.mil. The e-mail must include the following:

- Your name
- Your e-Mail
- Your phone
- Your organization and Location
- Your project name and government sponsor
- Technical POC name (*person receiving SDK*)
- Technical POC e-mail
- Technical POC phone

A request form will be sent, and once received back, upon approval, the SDK will be made available to download. Please allow one week for delivery of SDK. You will receive an email with a link to download the documents.

2.5.2 SDK Documentation

All documentation is releasable to the DoD and U.S. DoD contractors only. The following is the current list of SDK documents available:

- Architecture Description Document (ADD)
- Interface Design Description (IDD) - Core Only
- System-Subsystem Design Document (SDD)
- Universal CONOPS
- Quick Start Reference Guide
- Installation Guide

Other transition documents will include the following documents:

- Build procedures
- Software version description
- Business rules manual
- Software release notes

Contact Information

Operational Manager

EUCOM

Joe Fagan

Joe.e.fagan.civ@mail.mil

49 711 680-8955

Transition Manager

SPAWARSYSCENPAC

Doug Hardy

Douglas.hardy@navy.mil

619-553-5410

Deputy Transition Manager

GSE

Chris Russell

Chris.russell@globalsyseng.com

703-915-2338

Technical Manager/Performer

ARDEC

Italo Grasso

Italo.g.grasso.civ@mail.mil

973-724-8052

2.6 Keystone Authority to Operate (ATO)

The authority to operate for Keystone was approved effective 16 Jan 2014 with an Authorized Termination Date of 15 Jan 2017. This application is approved as a Type ATO at the MAC II/Sensitive level.

A Certificate of Networthiness (CoN) request was submitted on 19 Feb 2014. Keystone passed its Network Enterprise Technology Command (NETCOM) analyst review and is awaiting signature by the NETCOM approving official.

3 Transition Partners and Agreements

The EUCOM Keystone transition agreement outlines the terms under which EUCOM Keystone will be transitioned from the Product Agent to the Sustaining Agent (end user). Terms identified for agreement include:

- The select products to be delivered by the Product Agent.
- Any known gaps or shortfalls and their fixes (if possible) before the Sustaining Agent will accept the delivery.
- The acceptance events (e.g., TTX, Operational Demo) required by the Sustaining Agent to ensure product capability and readiness.
- A projected timeline for the final acceptance of the product by the Product Agent and Sustaining Agent.

3.1 Technology Transition Agreements (TTAs)

When the Keystone product is transitioned to a partner, the organization and USEUCOM sign an agreement that, among other things, details which product deliverable the partner will receive. This section lists each EUCOM Keystone Project partner and the proposed deliverables. After receiving the Product Deliverable package, the Transition Partner signs a Product Acceptance Letter/Transmittal Letter to complete the Transition Agreement.

3.1.1 Partners

ORGANIZATION	TRANSITION PARTNER	TRANSITION OWNER	TRANSITION AGREEMENT
JPEO CBD	Joint Project Manager Guardian (JPMG)	Ms. Karen House	Technology Transition Agreement (TTA) – JPMG through its programs and in conjunction with ARDEC is working to find a Keystone capability deployment strategy as the sustainment organization.
JPEO CBD	Joint Project Manager Information Systems (JPMIS) Joint Warning & Reporting Network (JWARN) Program of Record (POR)	Mr. Scott White	Technology Transmittal Letter – JPMIS through its programs, namely JWARN and Biosurveillance Portal (BSP), will work with JPMG and ARDEC to examine the feasibility of Keystone capability integrated into one of its program baselines.

NGB	National Guard Bureau (NGB)	Mr. Philip Cox	Technology Transmittal Letter – NGB is performing a pilot with the Joint Information Exchange Environment (JIEE), South Carolina and North Carolina using Keystone. They are interested in using the latest version from EUCOM Keystone for the pilot. Results from their pilot could provide excellent feedback for the EUCOM Keystone team.
PDC	Pacific Disaster Center (PDC)	Dr. Erin Hughey	Technology Transmittal Letter – PDC is interested in consuming data from the Keystone core into its DisasterAware program that provides all hazards situational awareness primarily for the PACOM and SOUTHCOM AORs.

3.1.2 Product Deliverables

KEYSTONE PRODUCT DELIVERABLE PACKAGE
Software
• Keystone Source Code[2] • Executables
Documentation
SDK Documents • Architecture Description Document (ADD) • Interface Design Document (IDD) – Core Only • System-Subsystem Design Document (SDD) • Universal CONOPS • Quick Start Reference Guide • Installation Guide
Information Assurance Documents • Army DIACAP Package • Army CoN Package • Army ATO (Authority to Operate)
Other Documents • Build Procedures • Software Version Description • Business Rules Manual • Software Release Notes • Test Procedures, Scripts, Scenarios, Data • Training Materials (Briefing Slides, Usage Scenarios)
Training/Product Support
• User Training • Product Support (Help Desk)

[2] In accordance with the ATO, ARDEC is responsible for the integrity of the software code. Therefore, the Keystone software code shall remain under ARDEC's Configuration Management Control.

4 Transition Acceptance Events

This section outlines Keystone's move from the science and technology (S&T) development stage to a product ready to be used in an operational environment: ready to prevent/respond to an incident or to alert/receive alerts from other partners. Acceptance events are increasingly operationally focused demonstrations and/or exercises intended to improve the transition readiness of the software to the receiving program. In the end, successful test and assessment reports will lead to a product acceptance letter between the TTA organizations, indicating the receiving program's intention of integrating the Keystone product.

4.1 USAG Stuttgart Discovery Meeting / Site Visit (Stuttgart, Germany – June 2014)

The EUCOM Keystone Team conducted the initial discovery meeting with USAG Stuttgart staff members to determine their processes and procedures during a response to a crisis.

4.1.1 Discovery Objectives

- Opportunity to assess USAG Stuttgart's (Panzer) current EM tools and procedures
- Focus areas for the site survey visit:
    - Current Garrison CONOPS/TTP/capabilities
    - Map data availability
    - Network/IT coordination
    - Host Nation coordination/capabilities
        - Baden-Wurttemburg Polizei Presidium
        - Baden-Wurttemburg Fire Department
        - Indications of policy issues
- Organizations who participated in the Site Survey:
    - USAG Stuttgart EM
    - MWR (facilities include hotel, gym, bowling center, outdoor recreation, auto crafts, CDC, sports office)
    - School Liaison
    - Clinic
    - AAFES (facilities include: PX, clothing store, laundromat, car care center, and school cafeteria)
    - Child and Youth Service / Child Development Center
    - Department of Public Works
    - Provost Marshal
    - Fire Chief

- Stuttgart City Control Center (Fire)
- Marine Forces Europe (MARFOREUR)

4.1.2 Discovery Findings

- Project was technically feasible – no IT roadblocks
- Current method for most communication was by phone (US/HN)
- No COP/Incident Management system was available for USAG Stuttgart to manage emergency services
  - Plan was to provide PSIF
- The common system for host nation EM / Fire was Geobyte
  - German state appeared to be addressing a similar problem to what Keystone addressed
  - GeoByte software subsequently purchased for integration
- Operationally, host nation fire/police were receptive
  - Must work through policy issues

4.2 Stallion Shake Exercise / Baseline Observations (Stuttgart, Germany – July 2014)

United States Army Garrison (USAG) Stuttgart held its annual Emergency Management exercise, Stallion Shake, on 29 July 2014 in Stuttgart, Germany. The EUCOM Keystone team was present to observe the exercise and understand the Concept of Operations, and to investigate potential opportunities to automate the information sharing aspects of the exercise. The exercise went as planned and the team had an opportunity to observe the "as is" configuration of USAG Stuttgart's emergency operations center (EOC).

4.2.1 Stallion Shake Observation Key Findings

- Only a small percentage of the population in USAG Stuttgart was covered by the current mass warning and reporting approach
- Most communication was by phone (US/HN), email, radio
- No COP across USAG Stuttgart used to manage emergency services (PowerPoint and Grease Boards represented the COP at the EOC, and hard copy maps and whiteboard represented the COP at the Mobile Incident Command)
- Incoming information was from the Military Police (MP) desk over the radio, and outgoing was a phone call to the EOC
- Laptops/monitors were not used (no email, mapping tools, etc.)
- Difficult to corroborate/verify information coming in, sometimes conflicting reports were received

Figure 4 depicts the current state of USAG Stuttgart EM and subsequently, the goal for a COP of EM event data and communications within the USEUCOM Keystone construct for this demonstration. The "as is" is represented by a system of grease boards, manual drawing and calculating, and "to be" will be fully functional electronic calculating, modeling and information sharing.

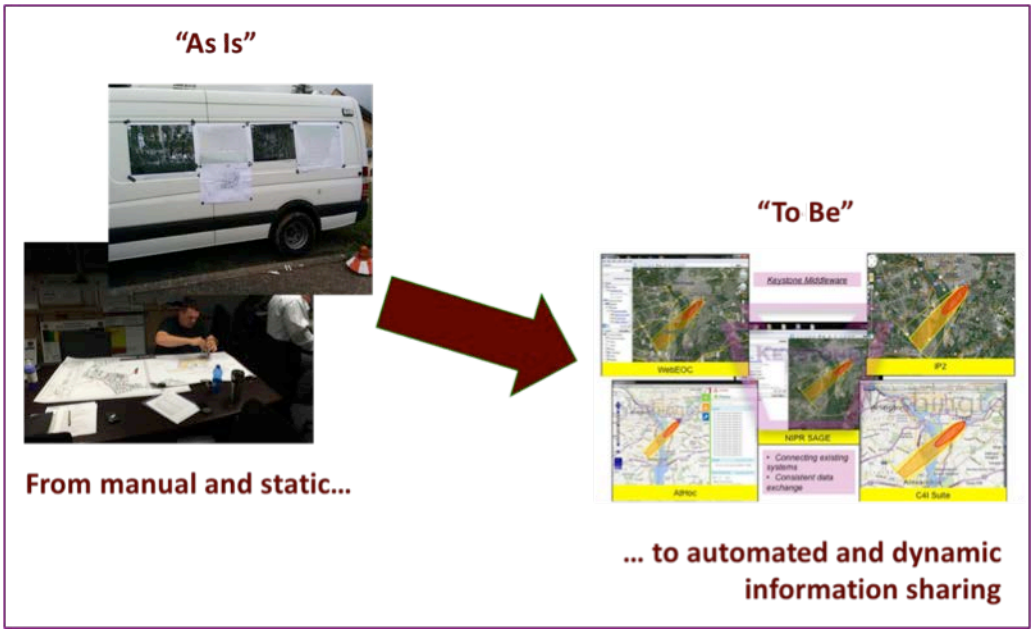


Figure 4: Current and future states of the EMS and information sharing capabilities at USAG Stuttgart

4.3 CONOPS Working Group (Picatinny, NJ – October 2014)

An information sharing CONOPS working group convened in October 2014 to discuss the initial, anticipated concept of operations and review potential business rules.

4.3.1 Working Group Focus Areas

- Information flow
- Incident reporting structure (MP, IOC, EOC)
- Directory of Emergency Services (DES) daily activities
- IOC daily activities
- Host nation considerations
- Training plan

4.3.2 Business Rules Outline

- EUCOM organization structure
- Daily operations (MP, DPTMS/IOC, Fire)
- Operations/Information flow during an incident
- Process/Rules for information sharing

- Keystone architecture for EUCOM
- PSIF dashboard

4.4 CONOPS Operational Validation (Picatinny, NJ – January 2015)

On 21-22 Jan 2015, the EUCOM Keystone Initial Capabilities Demonstration was held to review and validate a proposed EUCOM Keystone configuration and Concept of Operations (CONOPS) for day-to-day activities as well as critical incident situations.

4.4.1 Demonstration Objectives

- Illustrate the information-sharing process for EUCOM Keystone
- Exhibit the operational use of PSIF Dashboard by the MP desk, Fire and IOC
- Display a sample setup and operations of WebEOC for DES and DPTMS
- Show the AtHoc Mass Warning integration with the Dashboard
- Prove integration with the host nation GeoByte system

4.4.2 Demonstration Key Findings

- Keystone operated without any problems
- Participants were happy with the layout and basic operation of the dashboards
- Need CONOPS to figure out how to create, track, update resource requests from WebEOC
- GeoByte Keystone interface worked correctly; information shared by WebEOC was sent to Keystone and from there to GeoByte – the initial incident and updated information was received correctly
- USAG Stuttgart is going from a basic telephone-oriented communications approach to the use of an EMS and other capabilities including Keystone
- Alert notifications embedded in the system are required
- Casualty tracking needs to be shared between systems (GeoByte currently keeps an updated set of casualty information)
- Accountability notification and response should be added to the system

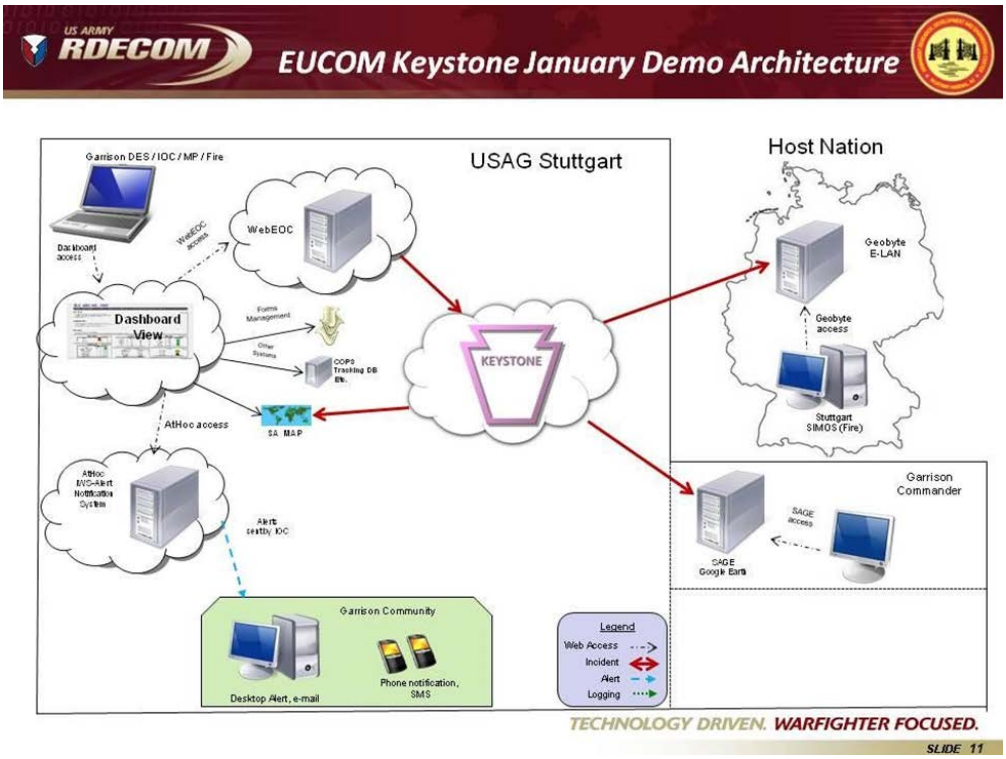


Figure 5: EUCOM Keystone CONOPS Demonstration Architecture

4.5 USAG Quarterly Exercise (Stuttgart, Germany – March 2015)

On 20 March 2015, a EUCOM Keystone capabilities exercise was held as an extension of the USAG March troop diversion exercise, which occurred on 19 March 2015. The Keystone team observed the operations and data flow at the EOC at Panzer Kaserne, which was staffed with the Ops and Planning groups to support the troop diversion exercise. These observations shaped the data flow for the 20 March Keystone exercise. This quarterly exercise was a full EOC exercise utilizing WebEOC as the EMS with Keystone operating to share the information with other systems.

4.5.1 Exercise Objectives

- Demonstrate EUCOM Keystone capabilities in the USAG Stuttgart environment
- Establish the ability to share WebEOC information with the Host Nation system, Higher Headquarters (HHQ), and Joint Operations Centers (JOC EUCOM, JOC AFRICOM)
- Understand how to integrate the Keystone WebEOC Board into the current USAG Stuttgart CONOPS

4.5.2 Exercise Key Findings

- Keystone system and adapters functioned correctly, reliably, and as required

- USAG Stuttgart is still learning how to use WebEOC but the basic data flow and roles have been defined
- There is now a good understanding of how to incorporate Keystone and the Keystone WebEOC board into Stuttgart CONOPS
- The Operations and Plans who were the key driving forces for the exercise were impressed with automatic sharing of Keystone to GeoByte and Google Earth
- The Garrison is still creating the CONOPS for the review and approval of information sharing

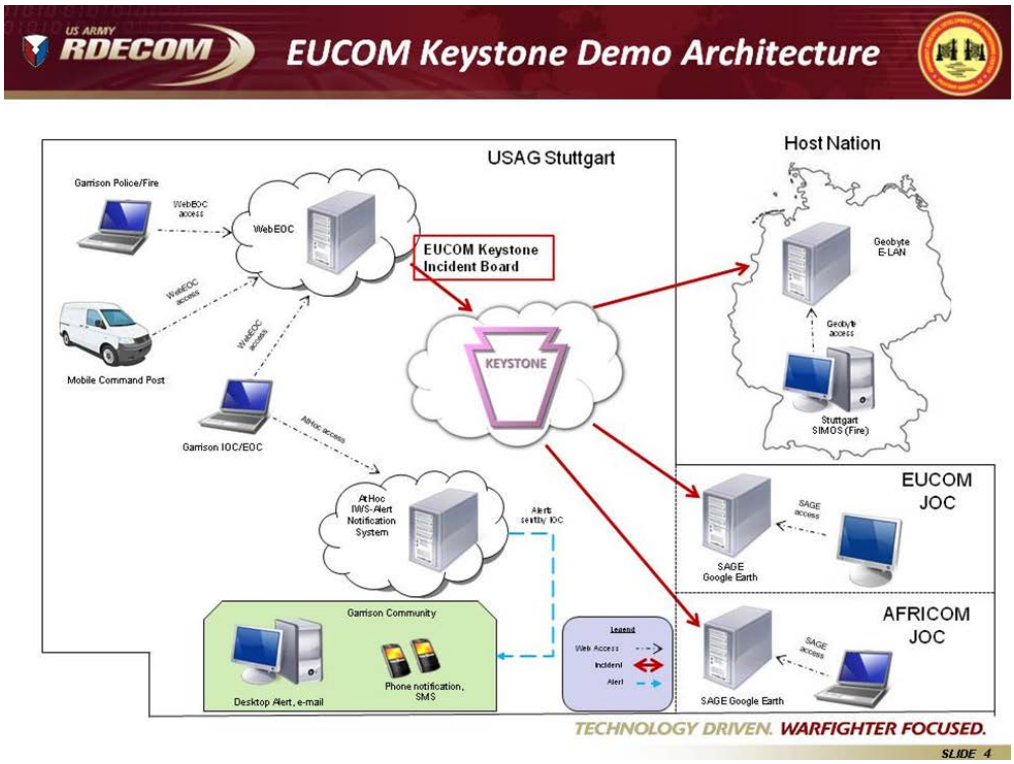


Figure 6: EUCOM Keystone Quarterly Exercise Architecture

4.6 Capabilities Assessment and Demonstration (Picatinny, NJ – August 2015)

The full capabilities assessment and demonstration of the EUCOM Keystone Project was completed in Picatinny, New Jersey, 24-28 Aug 2015. The objective of this demonstration was to show the full set of functionality that could be implemented in the EUCOM environment. Included was a technical assessment of the Keystone functionality to document the full set of capabilities available to EUCOM. The format of the demonstration was a simulated setup of the USAG Stuttgart/EUCOM environment and the systems shared information based on various scenarios that demonstrated the various competencies and possibilities using Keystone to share among the systems.

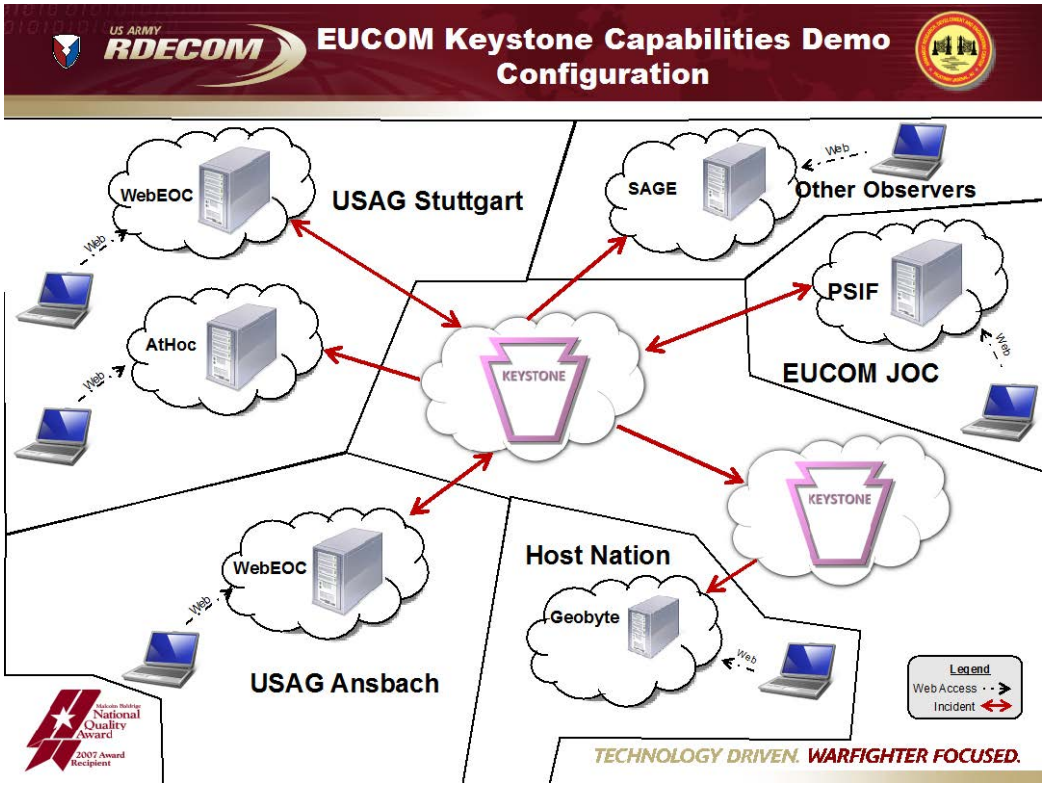


Figure 7: EUCOM Keystone Capabilities Demonstration Architecture

4.6.1 Capabilities Assessment

On 26 Aug 2015, the Keystone team conducted a capabilities assessment based on the completion of Software and Functional Testing the week prior. The Functional Testing served as the final test event prior to the upcoming demonstration in EUCOM at the U.S. Army Garrison, Stuttgart.

The functional testing resulted in no failures attributable to the EUCOM Keystone capabilities. The system was assessed as ready to conduct the field demonstration in EUCOM.

Figure 8: EUCOM Keystone verifying results during Capabilities Assessment

The following technical capabilities were verified as functional during controlled testing. 1) Keystone provided data transfer between the following end systems in accordance with their technical capabilities: WebEOC, AtHoc, Geobyte, PSIF, and SAGE. 2) Rule sets were validated with USAG Stuttgart CONOPS. 3) The Keystone Management Console provided the user a Graphical User Interface for configuring and managing the agreements and sharing rules, and permitted the user the ability to create and modify the list of Keystone Adapters that will be connected to the given Keystone Core.

During the assessment, three scenarios of varying degrees of difficulty were executed. The results of each scenario demonstrated a very consistent and extremely fast translation of information between disparate systems using Keystone. The end systems shared incident event information based on the Keystone sharing rules in seconds, typically 3-6 seconds.

4.6.2 Capabilities Demonstration

On Aug 27, the Capabilities Demonstration culminated in a presentation to numerous representatives from USNORTHCOM, PSEAG, EUCOM, AMC, JPM Guardian, JPM IS, SPAWAR Pacific, ECBC, National Guard Bureau, South Carolina National Guard, Picatinny DPTMS, and Picatinny Garrison Commander LTC Parker, several software vendors and ARDEC personnel. The Keystone team successfully demonstrated the system capabilities by utilizing an Emergency Management/Force Protection scenario developed by the US Army Garrison Stuttgart AT/FP office for Stuttgart's annual Full Scale Exercise "Stallion Shake." Keystone showed the ability to share information between several disparate EM systems in near-real time, that enhanced situational awareness and mission assurance during Prevention, Preparation, Response, and Recovery of an emergency event. Specifically

within the mock EUCOM environment, Keystone was shown to connect installation emergency management systems (as depicted in Figure 7) with the Host Nation emergency management system. A sandbox version of the live German system was used to demonstrate effective information sharing.

The power of Keystone middleware sharing information accurately and timely (near real time) was demonstrated in the Testbed Emergency Operations Center (TEOC) (see Figure 9) with operators on the various disparate systems sharing plume data after an exercise simulated explosion and fire on base.

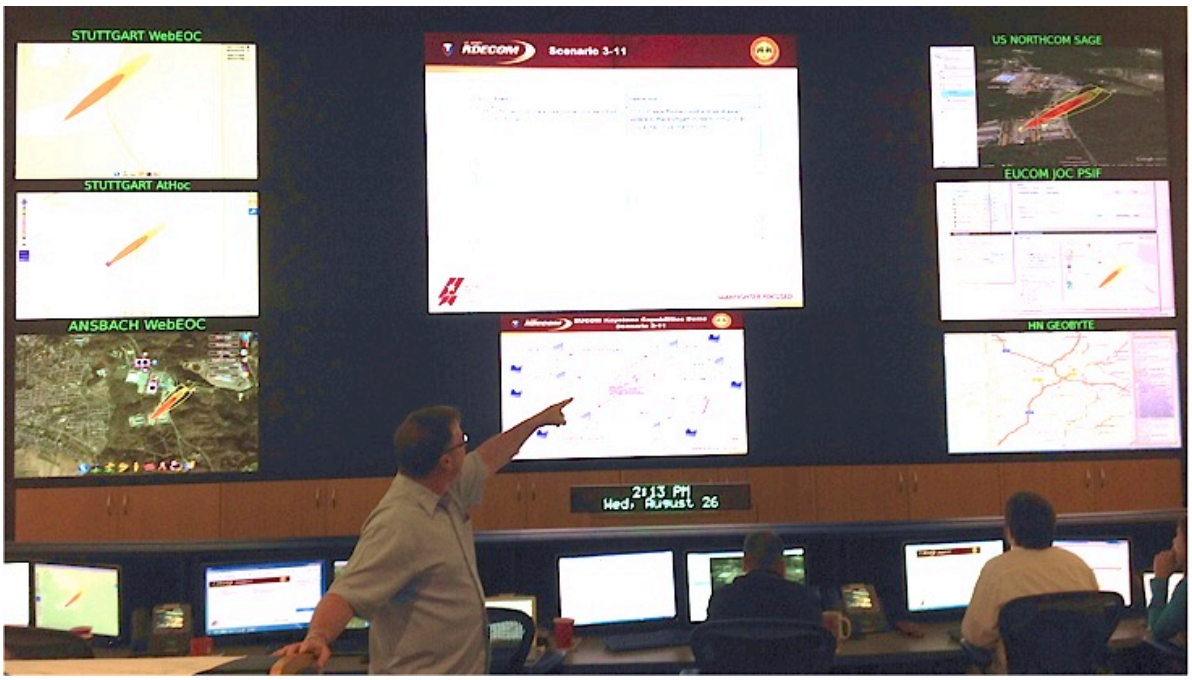


Figure 9: Joe Fagan, EUCOM Keystone OM, pointing to consistent Plume data during Capabilities Demo

The final results and assessment of the Capabilities Demonstration will be published as part of the overall Operational Utility Assessment (OUA) after the Stallion Shake Exercise in September 2015.

4.7 EUCOM Keystone Operational Demonstration as part of the Stallion Shake Exercise (Stuttgart, Germany – September 2015)

An Operational Demonstration (OD) of the EUCOM Keystone Project took place in Stuttgart, Germany, on 26 Sept 2015, as part of the USAG Stuttgart Stallion Shake Annual Emergency Management Exercise (see Figure 10).

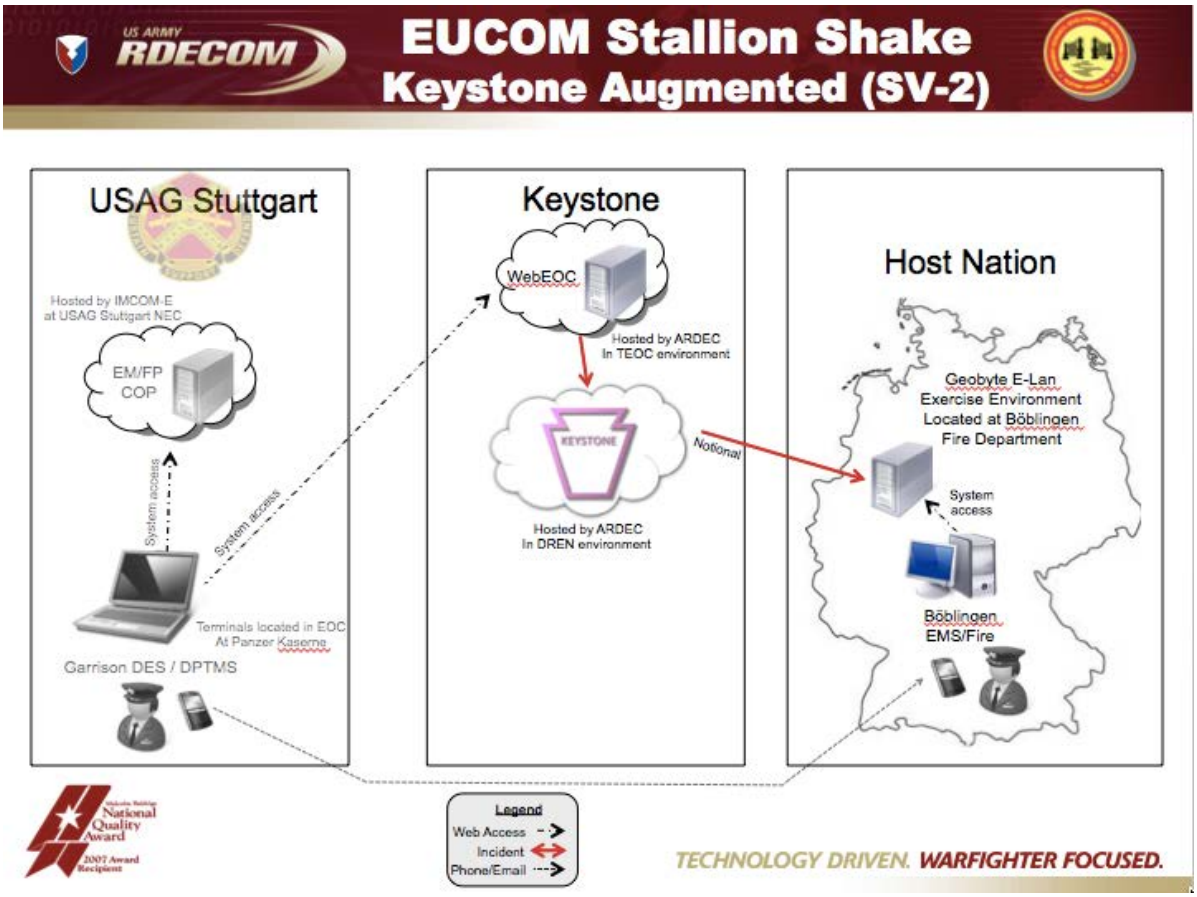


Figure 10: EUCOM Keystone System View for USAG Stuttgart "Stallion Shake" Exercise

The EUCOM Keystone project augmented the exercise and demonstrated the information sharing capabilities between the Garrison system (WebEOC) and the Host Nation system (GeoByte) using Keystone. The use of the Host Nation system, GeoByte (pictured in Figure 11 below), was a first time emergency management information sharing event between Germany and the USA Garrison.

The Garrison system (WebEOC) was used in the USAG HQ Emergency Operations Center (EOC). A EUCOM Keystone team member was co-located in the EOC and worked side-by-side with an EOC operator who provided event reporting in parallel on a second WebEOC instance enabled with Keystone (see Figure 12 below). Keystone then shared the event information with the Mobile Command Center system (WebEOC) and the Host Nation system (GeoByte). Information was shared back to the EOC and updates were exchanged by the systems.

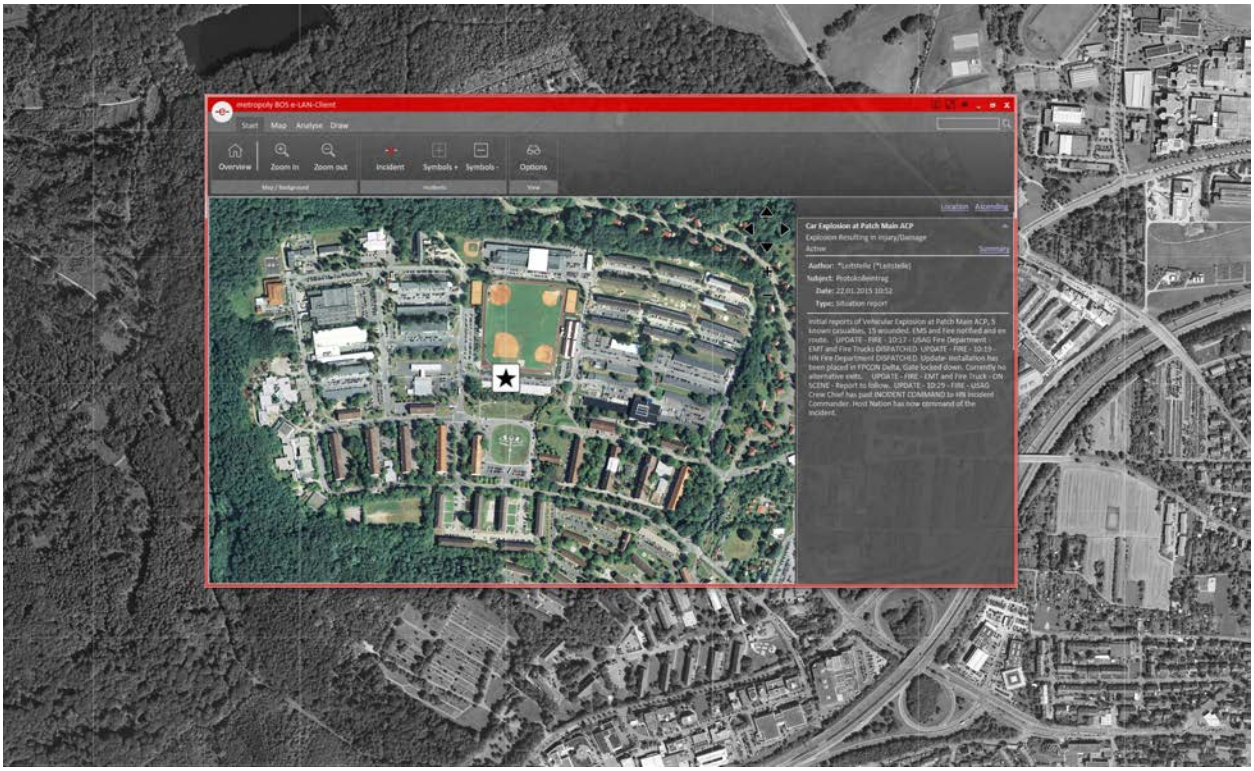


Figure 11: First time ever... GeoByte (Host Nation) system sharing data via Keystone with WebEOC located on the USA Garrison Mobile Command Center

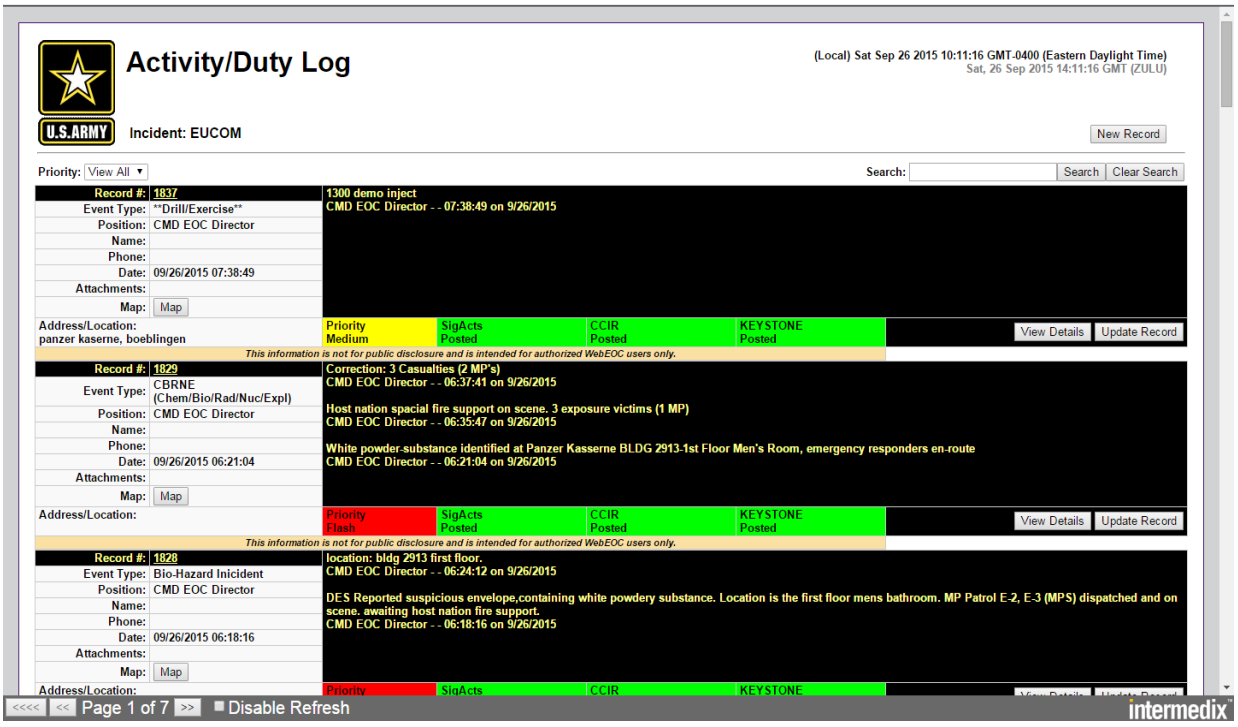


Figure 12: WebEOC Position Log in USAG EOC. WebEOC is enhanced with a Keystone Board for data sharing

4.7.1 The Annual Exercise "Stallion Shake"

The exercise included over twenty organizations, including five or more from the Host Nation. The objective of this exercise was to train for a real world emergency management scenario inclusive of an active shooter, a bomb detonation, a resulting fire and potentially threatening plume, and a suspicious letter with white powder.

Figure 13: USAG Incident Command Post area with German Fire Dept., German Police, German Red Cross, and USAG Mobile Command Center. A search Helicopter hovers near the top right of picture

On base an Incident Command Post (ICP) formed (Figure 13 above), and personnel from both Host Nation and USAG Emergency Responders began descending on the ICP to get updates and determine response posture. All emergency command vehicles used white-board like attachments to the sides of their vehicles to provide the latest situational awareness to the numerous emergency personnel on scene. The data on the status boards was largely populated by the EM systems operating within the vehicles, and those systems were sharing a common situational awareness via Keystone. The following pictures represent some of the activity at the ICP.

Figure 14: USAG Incident Command Post during Stallion Shake Exercise with Situation Board (USAG Mobile Command Center)

Figure 15: SGT Keller (left) operating Radios, WebEOC inside USAG Mobile Command Center

Figure 16: German Emergency Responders at USAG Stuttgart during Stallion Shake Exercise with Situation Board (German Fire Dept. Mobile Command Vehicle)

Figure 17: German Emergency Responders using GeoByte inside German Fire Dept. Mobile Command Vehicle

Figure 18: Long line of Host Nation Emergency Vehicles on Post during Stallion Shake Exercise

4.7.2 Exercise Key Observations

Key Observations (Garrison Stuttgart EOC)

- WebEOC in full use by EOC staff
- Second WebEOC instance with Keystone Board provides data to Mobile Incident Command Vehicle and Host Nation EM system
- Email and phones still necessary to communicate outside WebEOC

Key Observations (Mobile Incident Command Vehicle)

- WebEOC with Keystone enhanced information posted on large whiteboard for mission SA
- WebEOC (with Keystone Board) facilitated coordination of information with Garrison EOC

Key Observations (German Fire Department Command Vehicle)

- Keystone enabled first two-way exchange of information via an incident management system with a Host Nation system (GeoByte) and the Mobile Incident Command Vehicle (WebEOC)

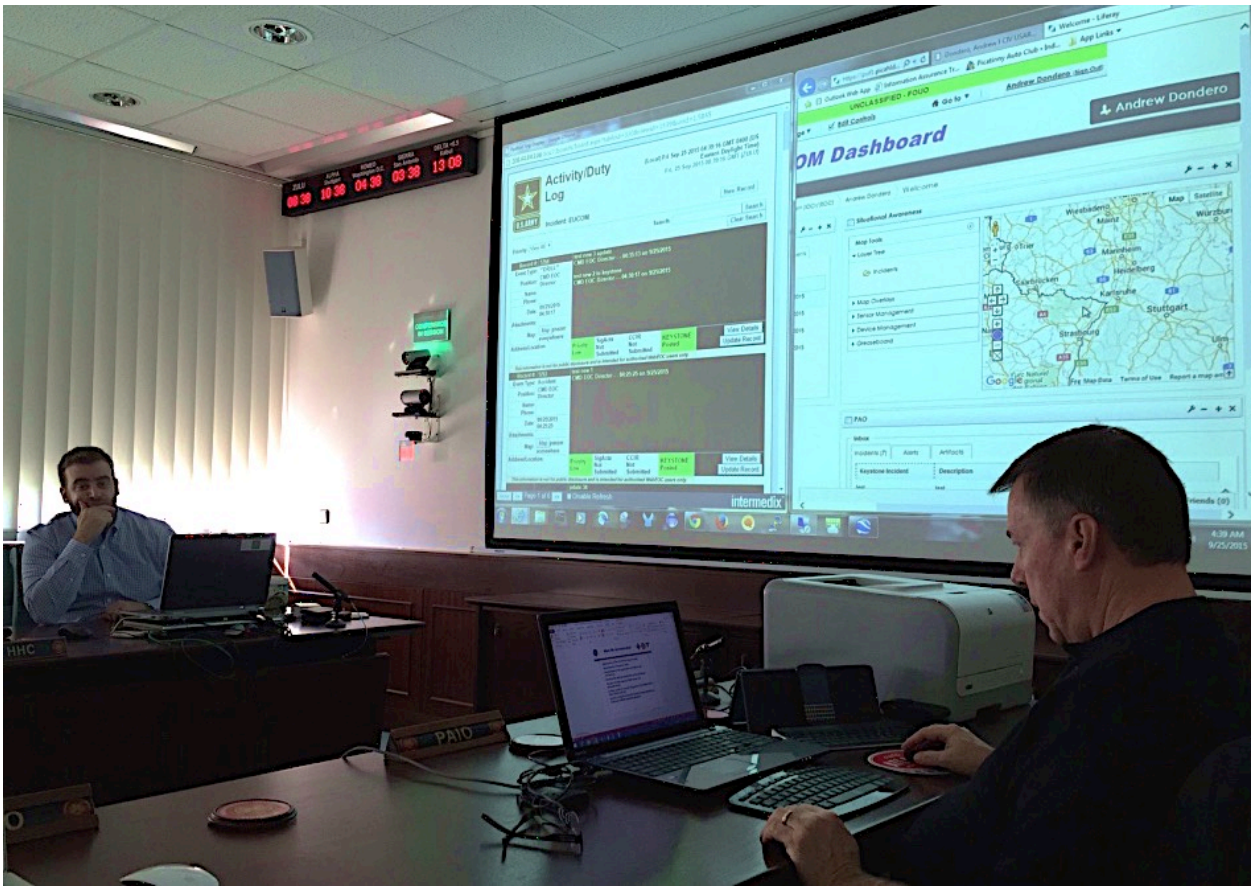


Figure 19: EUCOM Keystone team observing WebEOC and PSIF connected through Keystone to a WebEOC in the USAG EOC. [Pictured: Andrew Dondero (left), Joe Fagan (right)]

4.7.3 Exercise Assessment

The focus for the Keystone team was on the operational aspects of information sharing, how and when information was shared and its value to the participants. Near the end of the exercise timeline, a demonstration of the full capability was provided to the US Army Garrison Commander, Deputy Commander, and staff. In addition to WebEOC and GeoByte, the full capability demonstration included AtHoc, Physical Security Integration Framework (PSIF) and Situational Awareness Geospatial Enterprise (SAGE), very similar to the configuration at the Capabilities Demonstration as shown here in Figure 20.

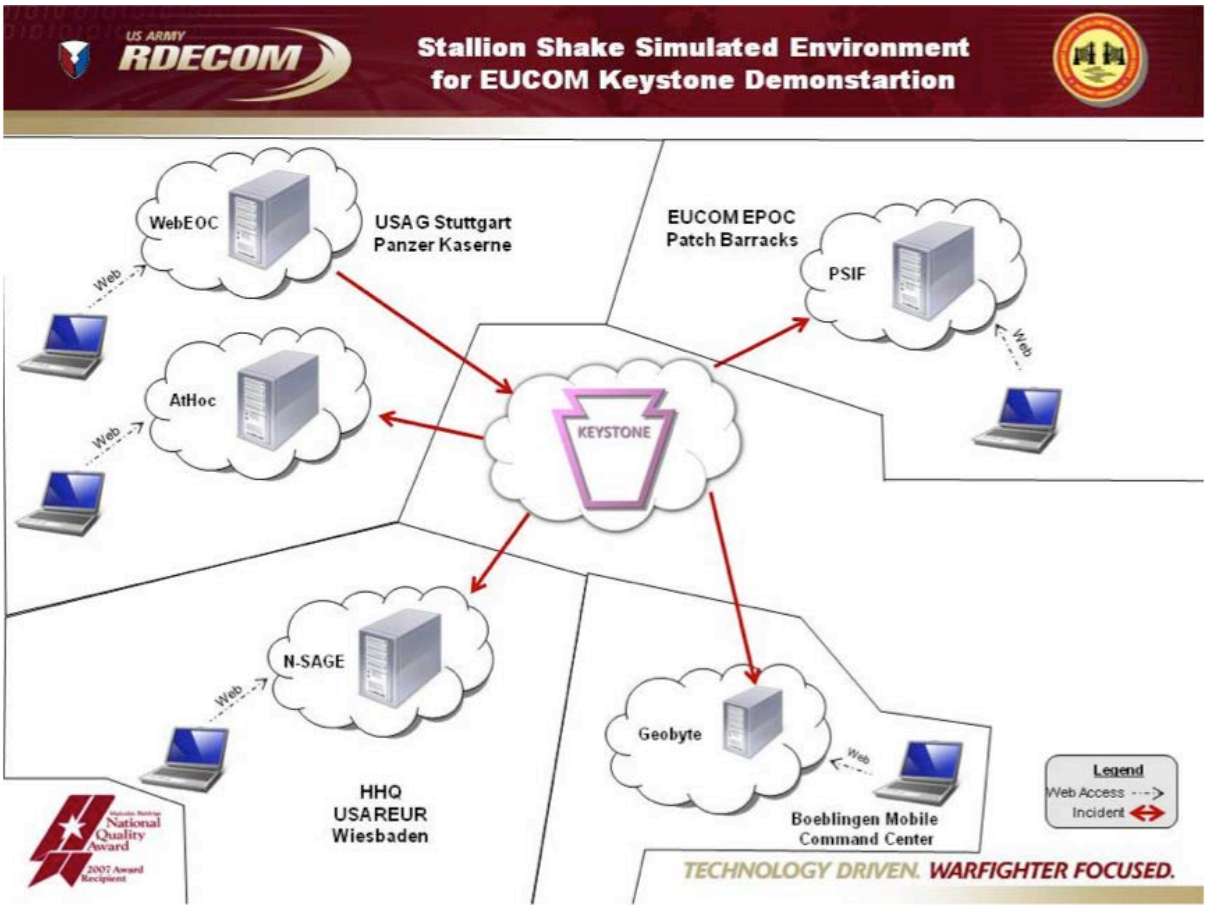


Figure 20: EUCOM Keystone Simulated System View for Full Capability Demonstration

The EUCOM Keystone team conducted an assessment using Host Nation, USAG Stuttgart capabilities, US Army Europe (USAREUR) representative systems and EUCOM representative systems. Initial results indicated that the data provided a much more common understanding of the operational picture on Post to both the Host Nation (Germany) and USAG Emergency Responders. The final results of the Operational Demonstration in September 2015, and the recent Capabilities Demonstration at Picatinny Arsenal in August 2015 will be published in the Operational Utility Assessment (OUA) report.

5 Other Transition Key Stakeholders

There are many organizations and efforts that have influenced the development of the EUCOM Keystone product. In addition to the requirements generated from the Fort Hood and Navy Yard shootings, we have additional stakeholders that have helped shape products, adjust business rules and provide considerations for new software adapters.

5.1 ODASD NM

The Office of the Deputy Assistant Secretary of Defense for Nuclear Matters (ODASD NM) is a sponsor for the EUCOM Keystone Project that provides oversight. Its mission is to achieve a world without nuclear weapons, sustain a safe, secure, and effective nuclear deterrent, and counter the threat from nuclear terrorism and nuclear proliferation.

5.2 JPEO CBD

The Joint Program Executive Office for Chemical and Biological Defense (JPEO CBD) is a stakeholder and transition partner for the EUCOM Keystone Project. It is the Joint Services single focal point for research, development, acquisition, fielding and life-cycle support of chemical and biological defense equipment and medical countermeasures.

5.3 USAG Stuttgart (Operational User)

The U.S. Army Garrison (USAG) Stuttgart is a stakeholder and transition recipient for the EUCOM Keystone Project. USAG Stuttgart is part of the Installation Management Command (IMCOM) that manages Army installations worldwide. One objective of USAG Stuttgart is to seek and maintain excellent working relationships with all Host Nation municipalities surrounding their installations.

5.4 ARDEC (Technical Manager)

The U.S. Army Armament Research, Development, and Engineering Center (ARDEC) serves as the Program Manager and Technical Manager for the EUCOM Keystone Project. ARDEC is an internationally acknowledged hub for the advancement of armament technologies and engineering innovation and strives to support the Army's efforts to ensure Soldier survivability and enhance platform and area protection by providing engineering, design, and development support.

5.5 SSC Pacific (Transition Manager)

The Space and Naval Warfare Systems Center (SPAWAR) Pacific serves as the Transition Manager for the EUCOM Keystone Project. Its mission is to enable Information Dominance

for our Naval, Joint, National and Coalition warfighters through research, development, delivery and support of integrated capabilities.

5.6 DHS S&T (Transition Partner)

The Keystone software originated with the Department of Homeland Security (DHS) Directorate of Science and Technology (S&T). They developed and fielded the Unified Incident Command and Decision Support (UICDS), a similar national information-sharing middleware, to share Common Operational Data (COD) and deliver information sharing in operational support of the National Incident Management System.

5.7 PDC

Pacific Disaster Center (PDC) is an applied science, information and technology center, working to reduce disaster risks and impacts on life, property, and the economies worldwide. PDC's products and services are used to support sound decision making in disaster response and civil-military humanitarian assistance operations, as well as in disaster risk reduction, mitigation and planning. In particular, PDC is a key provider of data and information services to USPACOM for natural and manmade disasters.

5.8 TaCBRD/EUCOM

The Transatlantic Collaborative Biological Resiliency Demonstration (TaCBRD) is a collaborative program between the U.S. Department of Defense (DoD), the U.S. Department of State (DOS), and the U.S. Department of Homeland Security (DHS). The Partner Nation for this program is the Republic of Poland. TaCBRD's objectives, with EUCOM representing the operational manager, are to develop and demonstrate a capability for resilience in countering a wide-area biological incident that impacts U.S. and Partner Nation civilian and military personnel and key infrastructure.

5.9 EUCOM EC J-8 (Operational Manager)

The United States European Command (EUCOM) EC J-8 serves as the Operational Manager for the EUCOM Keystone Project. The J5/8 develops basic military/political policy and planning for command activities involving relations with other U.S. combatant commands, allied and international military organizations, and subordinate commands. The J5/8 works closely with the other directorates, interagency partners and allies and uses diverse inputs to continually refine plans, ensuring they remain aligned with strategic guidance and the realities of an ever-changing environment. Whether it is evaluating current capabilities, searching for the next technological breakthroughs, or analyzing what EUCOM should look like in the next 10 years, the J5/8 always has its eyes on the future.

6 Other Related Events and Activities

6.1 Business Rules Working Group

The EUCOM Business Rules Working group is designed to establish the USAG Stuttgart Emergency Management organizations CONOPS, communications, and information flow in daily situations as well as during an emergency event. Subsequently, a set of information sharing rules for Keystone will be created.

ATTENDEES			
Name	Organization	Role	Contact Information
George Foley	ARDEC	Operations SME	George.b.foley.ctr@mail.mil
Chris Russell	GSE	Dep Transition Mngr	Chris.russell@globalsyseng.com
Sean Freeman	ARDEC	Key Participant	Sean.m.freeman14.civ@mail.mil
Andrew Dondero	ARDEC	Key Participant	Andrew.j.dondero.civ@mail.mil
Doug Hardy	SPAWAR PAC	Transition Manager	Hardydr@spawar.navy.mil
Joe Fagan	EUCOM	Operational Manager	Joe.e.fagan.civ@mail.mil
James Stoholski	ARDEC	Reviewer	James.r.stoholski.civ@mail.mil
Mike Cazzola	ARDEC	Reviewer	Michael.w.cazolla.civ@mail.mil
Kieth Reed	USA ERDC	Assessment Lead	Kieth.reed@censeoinsight.com

6.2 Assessment IPT

An assessment integrated product team (IPT) was established in October 2014, to provide a cross-coordinated focus working group to shape the assessments proposed through an independent assessment and OUA report. Functional and software testing was scheduled to be conducted and documented in accordance with the ARDEC software test plan just prior to the Technical Capabilities Demonstration, 24-28 Aug 2015. Further included in this demonstration was a technical assessment of the Keystone functionality as it applied to implementation within the EUCOM environment. In September 2015, the Stallion Shake field demonstration was conducted to demonstrate and assess the operational utility of the

EUCOM Keystone capabilities in a representative operational environment utilizing representative users.

The goal of the technical assessment was to identify the degree to which system capabilities supported operational activities. Further, it determined the degree to which operationally focused documentation supported the mission and associated tasks, and included what technical documentation was available, complete and accurate. Finally a preliminary technology readiness level (TRL) was assigned. The details of the preliminary TRL assessment will be available in the final OUA report. However, based on the functional and software testing, and the capabilities assessment and demonstration an initial TRL-7 was recommended and reflected in this publication.

The goal of the software and functional assessment was to evaluate and assess system functions in a laboratory environment, review code, databases, interface requirements and architecture. Issues discovered during functional evaluation were documented, troubleshooting was conducted, and potential risks were identified and evaluated. Issues from the capabilities assessment and demonstration events will be reported in the final OUA report.

Finally, the operational assessment team observed the operational demonstration event in Stuttgart, conducted group after action sessions, and administered surveys to participants on the use of representative technology in performing their tasks. Issues from the operational demonstration event will be identified and documented in the OUA report.

6.3 Assessment Plans and Reports

This product reference guide contains some preliminary results, but was submitted prior to the results of many of the assessment reports becoming available in October 2015. Information is available by request. Please contact Kieth Reed (kieth.reed@censeoinsight.com) or Andrew Dondero (andrew.j.dondero.civ@mail.mil).

The following is the summary list of EUCOM Keystone Assessment Documents available:

1. Demonstration Execution Document (DED)

   The EUCOM Keystone DED serves as the detailed event description for the demonstration of the EUCOM Keystone program. This DED describes the approach for management and analysis of data from the demonstration in EUCOM along with the software testing required prior to the demonstration in EUCOM. The DED describes the organization of the demonstration, the details of the data collection efforts during the event, the data management system, and other outstanding data management issues as they might impact the overall assessment strategy.

2. Operation Utility Assessment (OUA)

The EUCOM Keystone OUA reports on the assessment of the overall impact of the EUCOM Keystone program. The OUA Report serves as the capstone reporting document for the assessment team tasked to provide an OUA of the EUCOM Keystone CONOPS, tactics, techniques and procedures (TTP), and capability solution. The OUA also provides the necessary data to draw conclusions about utility and make decisions regarding technology improvements, technology discontinuance, or technology fielding. The OUA addresses software testing, one functional demonstration, and one field event designed to provide subjective and objective data, and to provide results to understand the impact and resolution of the following operational issues (OIs). The OIs were developed in coordination with the EUCOM user community.

OPERATIONAL ISSUE (OI) 1: How does EUCOM Keystone impact Force Protection (FP) / Emergency Management (EM) mission-support capabilities?

OPERATIONAL ISSUE (OI) 2: Does EUCOM Keystone provide automated, unclassified data sharing between users of U.S. Government and Host Nation situational awareness systems?

OPERATIONAL ISSUE (OI) 3: Is the EUCOM Keystone system suitable and sustainable with the existing and planned operational infrastructure and networks?

The OUA will also discuss the recommended technology readiness level based on software definitions and criteria for evaluating technology maturity. The final OUA report is anticipated in October 2015.

Appendix A: Acronyms

ACRONYM	DEFINITION
AAFES	Army and Air Force Exchange Service
ADD	Architecture Design Document
AMC	Army Materiel Command
AOR	Area of Responsibility
API	Application Programming Interface
ARDEC	Armament Research, Development and Engineering Center
ARNORTH PMO	Army North Provost Marshall's Office
ASD-NM	Assistant Secretary of Defense for Nuclear Matters
ATO	Authority to Operate
C2PC	Command and Control Personal Computer
C4IS	Command, Control, Communication, Computers, and Intelligence Suite
CAD	Computer-Aided Dispatch
CAP	Common Alerting Protocol
COD	Common Operational Data
CoN	Certificate of Networthiness
CONOPS/CONEMP	Concept of Operations/Concept of Employment
COP	Common Operating Picture
DED	Demonstration Execution Document
DES	Directorate of Emergency Services
DHS	Department of Homeland Security
DIACAP	Department of Defense Information Assurance Certification and Accreditation Process
DISA	Defense Information Systems Agency
DLA	Defense Logistics Agency
DoD	Department of Defense
DOS	Department of State

ACRONYM	DEFINITION
DOTMLPF-P	Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, and Facilities and Policy
DPTMS	Directorate of Plans, Training, Mobility & Security
DSEA	Defense Security Enterprise Architecture
DTA	Data Transition Agreements
DTRA	Defense Threat Reduction Agency
DTIC	Defense Technical Information Center
E2E	End-to-end
ECBC	Edgewood Chemical Biological Center
EDXL	Emergency Data Exchange Language
EM2P	Emergency Management Modernization Program
EM/FP	Emergency Management/Force Protection
EMS	Emergency Management System
EOC	Emergency Operations Center
ERDC	Engineer Research & Development Center — Geospatial Research Lab
ESB	Enterprise Service Bus
FEMA	Federal Emergency Management Agency
FOB	Forward Operating Base
FXD	Final Transition Demonstration
GIS	Geographic Information System
GOTS	Government Off-the-Shelf
HHQ	Higher Headquarters
HN	Host Nation
HTTPS	Hypertext Transfer Protocol Secure
IAP	Incident Action Plan
IATO	Interim Authority to Operate
ICD	Interface Control Document
ICP	Incident Command Post
ICS	Incident Command System

ACRONYM	DEFINITION
IDD	Interface Design Document
IMCOM	Installation Management Command
I/NGO	International and Non-Governmental Organizations
IOC	Incident Operations Center
IPAWS	Integrated Public Alert and Warning System
IPL	Integrated Priority List
IPT	Integrated Product Team
IT	Information Technology
IV&V	Independent Verification and Validation
IWS	Integrated Web Services
JAR	Java Archive
JAXB	Java API for XML Binding
JEM	Joint Effects Model
JIEE	Joint Information Exchange Environment
JITC	Joint Interoperability Test Command
JMS	Java Messaging Services (Java API)
JOC	Joint Operations Center
JPEO CBD	Joint Program Executive Office for Chemical and Biological Defense
JPM	Joint Project Manager
JPMG	Joint Project Manager Guardian
JPMIS	Joint Project Manager Information Systems
JTAG	Joint Test Assessment Group
JWARN	Joint Warning and Reporting Network
KML	Keyhole Markup Language
MAA	Mutual Aid Agreement
MAC II	Mission Assurance Category Level II
MARFOREUR	United States Marine Corps Forces, Europe
MATADRR	Mission Assurance, Threat Alert, Disaster Resiliency and Response

ACRONYM	DEFINITION
MOU	Memorandum of Understanding
MP	Military Police
MWR	Morale, Welfare and Recreation
NETCOM	Network Enterprise Technology Command
NCR	National Capital Region
NEO	Networked Emergency Operations
NGB	National Guard Bureau
NIEM	National Information Exchange Model
NIMS	National Incident Management System
NIPR	Non-Secure Internet Protocol Router
OASIS	Organization for the Advancement of Structured Information Standards
OCONUS	Outside Continental U.S.
ODASD NM	Office of the Deputy Assistant Secretary of Defense for Nuclear Matters
OI	Operational Issues
OM	Operational Manager
OUA	Operational Utility Assessment
PDC	Pacific Disaster Center
PM	Program Manager
POC	Point of Contact
POR	Program of Record
PRG	Product Reference Guide
PSEAG	Physical Security Enterprise & Analysis Group
PSIF	Physical Security Integration Framework
PUB/SUB	Publish and Subscribe
REST	Representational State Transfer
S&T	Science and Technology
SA	Situational Awareness
SAGE	Situational Awareness Geospatial Enterprise

ACRONYM	DEFINITION
SDD	System-Subsystem Design Document
SDK	Software Development Kit
SEIWG	Security Equipment Integration Working Group
SME	Subject Matter Expert
SOA	Service Oriented Architecture
SOAP	Simple Object Access Protocol (XML protocol)
SPAWAR	Space & Naval Warfare Systems Command
SSL	Secure Sockets Layer
SVD	Software Version Description
TaCBRD	Transatlantic Collaborative Biological Resiliency Demonstration
TCP	Transmission Control Protocol
TD	Technical Demonstration
TEOC	Testbed Emergency Operations Center
TM	Technical Manager
TNT	Technology and Transition
TRL	Technology Readiness Level
TTA	Technology Transition Agreement
TTP	Tactics, Techniques and Procedures
TTX	Table Top Exercise
UICDS	Unified Incident Command and Decision Support
USAG	U.S. Army Garrison
USAFRICOM / AFRICOM	U.S. African Command
USEUCOM / EUCOM	U.S. European Command
USMTF	United States Message Text Format
USNORTHCOM / NORTHCOM	U.S. Northern Command
USPACOM / PACOM	U.S. Pacific Command
WDSL	Wireless Digital Subscriber Line

ACRONYM	DEFINITION
WebEOC	Web Based Emergency Operations Center
XM	Transition Manager
XML	Extensible Markup Language

Appendix B: Key Stakeholder & Partner POC Information

Name	Organization	Email Address
Joe Fagan	EUCOM J-8	joe.e.fagan.civ@mail.mil
Shay Edwards	USAG Stuttgart HQ	shay.edwards.civ@mail.mil
Len Fagan	USAG Stuttgart DES Fire	leonard.j.fagan2.ln@mail.mil
SGT Branden Beene	USAG Stuttgart DES MP	brandon.w.beene.mil@mail.mil
Mark Keller	USAG Stuttgart DES MP	mark.d.keller20.civ@mail.mil
Bill Newman	Army G34	william.c.newman4.civ@mail.mil
COL James Choung	JPM Guardian	james.k.choung.mil@mail.mil
Don Buley	JPM Guardian	donald.c.buley.civ@mail.mil
Karen House	JPM Guardian	karen.m.house.civ@mail.mil
Erin Hughey, PhD	Pacific Disaster Center	ehughey@pdc.org
John Salley	USAF	john.t.salley.civ@mail.mil
Scott White	JPM Information Systems	sawhite@spawar.navy.mil
David Godso	JPM Information Systems	david.w.godso.civ@mail.mil
Andy Hill	JPM Information Systems	andyhill@spawar.navy.mil
Phil Cox	National Guard Bureau	phillip.r.cox1.civ@mail.mil
COL Brenda Mason	National Guard Bureau	brenda.f.mason.mil@mail.mil
MAJ Latonya Robinson	National Guard Bureau	latonya.s.robinson.mil@mail.mil
MAJ Ramel Jackson	National Guard Bureau	ramel.d.jackson.mil@mail.mil
David Acevedo	AtHoc	dacevedo@athoc.com
Italo Grasso	ARDEC	italo.g.grasso.civ@mail.mil
Andrew Dondero	ARDEC	andrew.j.dondero.civ@mail.mil
Bob Giarratano	ARDEC	robert.m.giarratano.civ@mail.mil
George Foley	ARDEC	george.b.foley.ctr@mail.mil
Kieth Reed	OM Support	kieth.reed@censeoinsight.com
Doug Hardy	SPAWAR PAC	hardydr@spawar.navy.mil
Chris Russell	OM/PM/XM Support	chris.russell@globalsyseng.com
Patricia Hile	OM/PM/XM Support	patricia.collett.hile@globalsyseng.com
Maj Gen David Allvin	EUCOM J-5 Director	david.w.allvin.mil@mail.mil
Jorge Zambrana	USNORTHCOM S&T	jorge.v.zambrana.civ@mail.mil
Jay Huston	USNORTHCOM S&T	jay.c.huston.civ@mail.mil
Tom Whittle	PSEAG	thomaswhittle48@gmail.com
Rod Gillis	PSEAG	roderick.e.gillis.civ@mail.mil

Postscript

The Transition Support Team would like to thank all contributors to this document. Even though the PRG was submitted prior to publication of the final assessment report, we hope you found valuable information about the product and who to contact as the product matures. If you have feedback or ideas on how to improve this report, or have general questions or comments about the project, or specific products named herein, please email: peggy.west@navy.mil or call: 619-553-6899. For an alternate point of contact, please email: douglas.hardy@navy.mil or call: 619-553-5410.

Primary Authors:

Douglas Hardy, EUCOM Keystone XM, SPAWAR Systems Center Pacific (SSC PAC)
Christopher Russell, EUCOM Keystone XM/TM Support, SSC PAC Contractor Support
Patricia Hile, EUCOM Keystone XM/TM Support, SSC PAC Contractor Support

Chief Editor:

Peggy West, EUCOM Keystone XM Support, SSC PAC

Publishers:

Art Armendariz, SSC PAC
Norman Tancioco, SSC PAC

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-01-0188

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
September 2015	Final	

4. TITLE AND SUBTITLE

EUCOM Keystone: Connecting Across Services Enabling Timely Horizontal & Vertical Integration, **Product Reference Guide**, Revision 1

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHORS

Douglas R. Hardy
SSC Pacific

Christopher E. Russell
Patricia C. Hile
Global Systems Engineering
G2 Software Systems, Inc.

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

SSC Pacific, 53560 Hull Street, San Diego, CA 92152–5001

8. PERFORMING ORGANIZATION REPORT NUMBER

TD 3299

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Office of the Deputy Assistant Secretary of Defense for Nuclear Matters
OASD(NCB/NM)
3050 Defense Pentagon (Room 3B884)
Washington, DC 20301-3050

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

This document describes the EUCOM Keystone products and related non-material solutions. Further, this document provides information for obtaining Keystone products and support. Lastly, the document contains artifact information for use in the Defense Technical Information Center (DTIC) for future programs and products.

15. SUBJECT TERMS

Mission area: Information Sharing
EUCOM Keystone
transition products
transition partners and agreements
transition acceptance events
assessment and demonstration

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Douglas R. Hardy
U	U	U	U	64	19B. TELEPHONE NUMBER *(Include area code)* (619) 553-5410

INITIAL DISTRIBUTION

84300	Library	(2)
85300	Archive/Stock	(1)
53627	D. R. Hardy	(50)

Defense Technical Information Center
Fort Belvoir, VA 22060–6218 (1)


SHARED MODE
ACCESS POINT
SHARED MODE
SHARED MODE
ACCESS POINT
ACCESS POINT
SHARED MODE
SHARED MODE


HEADQUARTERS
United States European Command